Cassandra Crossing/ La fine del mondo, virtuale

(576)—Sarà un bug informatico usato come arma a provocare la fine del mondo? Per adesso sappiamo che poteva succedere nel mondo virtuale…

Cassandra Crossing/ La fine del mondo, virtuale

Figure 1: Dr. Strangelove trailer from 40th Anniversary Special Edition DVD, 2004, Quest'opera è nel pubblico dominio perché pubblicata negli Stati Uniti fra il 1929 e il 1977, inclusi, senza un avviso di copyright. https://commons.wikimedia.org/w/index.php?curid=11862639

(576)—Sarà un bug informatico usato come arma a provocare la fine del mondo? Per adesso sappiamo che poteva succedere nel mondo virtuale, e che stavolta è andata bene. Ma domani?

7 marzo 2024 —

CVE-2024–22252–3–4–5.

Quando scritto qui sopra da Cassandra è incomprensibile al 99,9% delle persone normali, e probabilmente anche ai suoi 24 intelligentissimi lettori.

Tradotto in italiano, con una buona traduzione, di quelle che spiegano il significato più profondo, suonerebbe così:

"*Abbiamo evitato che qualcuno potesse provocare la fine del mondo delle macchine virtuali*".

Ma ancora per molti non sarà chiaro, od almeno non ne sarà chiara l'importanza. Riproviamo.

"*La maggior parte dei server al mondo potevano essere bloccati o distrutti da un singolo atto di guerra informatica, ma questa volta ce ne siamo accorti e l'abbiamo impedito*".

Chiaro, no? E veniamo al fatto.

CVE-2024–22252–3–4–5 è il nome assegnato ad una serie di falle informatiche che consentono di penetrare l'ipervisore dei sistemi VMware ESX, permettendo di accedere al server fisico sottostante, e di fare qualsiasi cosa, incluso bloccare o "*distruggere*" il server fisico, e con esso tutte le macchine virtuali che vi girano sopra.

Non molti sanno che la maggior parte dei server che costituiscono il tessuto della Rete odierna non sono "*ferro*", macchine fisiche, ma "*macchine virtuali*" che funzionano tutte insieme su un unico server specializzato. Diciamo tipicamente 10–100 macchine che condividono un unico computer.

Questi server sono forniti da pochissime ditte specializzate, e VMware è quella che detiene la fetta di mercato maggiore.

Il "*baco*" di cui stiamo parlando è relativo non ad un particolare prodotto della VMware, ma all'emulazione del sottosistema USB, che è incluso in tutti i prodotti dell'azienda, e che quindi può essere usato per comprometterli anche tutti insieme.

Uno zero-day di questo calibro potrebbe essere usato da un fabbricante di malware, o da un attore di uno stato-nazione che volesse dotarsi di un'arma informatica devastante dal punto di vista *tattico*, a livello della "*Macchina Fine del Mondo*" del "*Dottor Stranamor*e". Qualcuno ha detto *Stuxnet*?

Per fortuna non è successo.

Ma magari quest'arma era davvero già stata prodotta, e messa da parte per un uso futuro in qualche arsenale di Cyber-armi.

Per fortuna stavolta sarà disinnescata completamente nel giro di pochi giorni, e diverrà inutile come una bomba atomica privata delle semisfere di plutonio.

Non è quindi successo che una parte sostanziale del mondo reale smettesse di funzionare improvvisamente, magari innescando quel "Collasso" di cui Cassandra ama vaticinare da un po' di tempo a questa parte.

Ma quante di queste vulnerabilità esistono che non sono state ancora trovate?

E quante di queste sono in realtà state trovate e mai rese pubbliche, ma usate per confezionare altre Armi Cibernetiche, altre "*Macchine Fine del Mondo*" immagazzinate nei Cyber-arsenali di stati-nazione, canaglie o meno, di organizzazioni criminali, aziende di armamenti e compagnia cantando?

Tutto questo vi preoccupa o magari addirittura vi spaventa? Bene, vuol dire che siete ancora vivi e vigili.

E' notizia di questi giorni che il Presidente degli Stati Uniti ha ordinato ai programmatori che lavorano per il suo paese di smettere di usare certi linguaggi ed usarne altri, perché producono meno bug informatici. Dico, lui è preoccupato; sì, il Presidente degli Stati uniti si preoccupa di come lavorano i programmatori, dei danni che possono fare.

Voi cosa pensate di fare?

E per chiudere e non farvi dormire stanotte, Cassandra rincara la dose; questo tipo di problema, volendo preoccuparsi di catastrofi, non è il peggio che possa accadere. Vogliamo parlare di *silicio*? Esatto, e lo faremo.

Ma questa … questa è un'altra storia.

"*Stateve accuorti*"

Scrivere a Cassandra—Twitter—Mastodon
Videorubrica "Quattro chiacchiere con Cassandra"
Lo Slog (Static Blog) di Cassandra
L'archivio di Cassandra: scuola, formazione e pensiero

By Marco A. L. Calamari on March 7, 2024.

Canonical link

Exported from Medium on August 27, 2025.